CSfC Selections for Mobile Platforms

Mobile Platforms used in CSfC solutions shall be validated by NIAP/CCEVS or CCRA partnering schemes as complying with the current requirements of NIAP's Mobile Device Fundamentals Protection Profile. This validated compliance shall include the selectable requirements contained in this document.

CSfC selections for Mobile Device Fundamentals version l.x evaluations:

FCS_CKM.l .l (l): The TSF shall generate asymmetric cryptographic keys used for key establishment in
accordance with:

- *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" tor elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and[selection: P-521, no other curves[(as defined in FIPS PUB 186-4, "Digital Signature Standard")*

FCS_CKM.1.1(2): The TSF shall generate asymmetric cryptographic keys used for authentication in accordance with a specified cryptographic key generation algorithm

- *FIPS PUB 186-4, "Digital Signature Standard {DSS)", Appendix 8.4 for ECDSA schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves]*

FCS_CKM_EXT.l.l: The TSF shall support a hardware-protected REK with an AES key of size [256 *bits]*.

FCS_CKM_EXT.2.1: All DEKs shall be randomly generated with entropy corresponding to the security strength of AES key sizes of [256] bits.

FCS_CKM_EXT.3.1: All KEKs shall be *[256-bit]* keys corresponding to at least the security strength of the keys encrypted by the KEK.

FCS_COP.1.1(1): The TSF shall perform *[encryption/decryption]* in accordance with a specified cryptographic algorithm

- AES-CBC {as defined in NIST SP 800-38A) mode,
- AES-CCMP (as defined in FIPS PUB 197, NIST SP 800-38C and IEEE 802.11-2012).
- *AES-GCM (as defined in NIST SP 800-38D),* and cryptographic key sizes 128-bit key sizes and *[256-bit key sizes]*.

FCS_COP.1.1(2): The TSF shall perform *[cryptographic hashing]* in accordance with a specified cryptographic algorithm SHA-1 and *[SHA-256, SHA-384]* and message digest sizes 160 and [256, *384]* that meet the following: *[FIPS Pub 180-4]*.

FCS_COP.1.1(3): The TSF shall perform *[cryptographic signature services (generation and verification)]* in accordance with a specified cryptographic algorithm

- *FIPS PUB 186-4, "Digital Signature Standard (DSSJ", Section 5 tor ECDSA schemes and implementing "NIST curves" P-256, P-384 and {selection: P-521, no other curves/*

FCS_RBG_EXT.1.2: The deterministic RBG shall be seeded by an entropy source that accumulates entropy from *[TSF-hardware-based noise source]* with a minimum of [256 *bits]* of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

FCS_TLS_EXT.2.1: The TSF shall implement one or more of the following protocols TLS 1.2 (RFC 5246) and [selection: TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346)] supporting the following ciphersuites:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

FOP OAR_EXT.1.2: Encryption shall be performed using DEKs with AES in the [selection: *XTS, CBC,* GCM] mode with key size [256] bits.

FOP IFC_EXT.1.1: The TSF shall [selection: provide an interface to VPN applications to enable *all IP traffic (other than IP traffic required to establish the VPN connection) to flow through the IPsec VPN client,* enable *all IP traffic (other than IP traffic required to establish the VPN connection) to flow through the IPsec VPN client]*.

FIA_XS09_EXT.2.2: When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [selection: *allow the administrator to choose whether to accept the certificate in these cases, not accept the certificate]*.

FMT_MOF.1.1(2): The TSF shall restrict the ability to perform the functions [

1. configure password policy:
    a. minimum password length
    b. minimum password complexity
    c. maximum password lifetime
2. configure session locking policy:
    a. screen-lock enabled/disabled
    b. screen lock timeout
    c. number of authentication failures
3. enable/disable [assignment: list of audio or visual collection devices]
4. configure application installation policy by [selection:
    a. specifying authorized application repository(s),
    b. specifying a set of allowed applications and versions (an application whitelist)
    c. denying installation of applications],
5. enable/disable the VPN protection
9. specify wireless networks (SSIDs) to which the TSF may connect]

FMT_SMF.1.1: The TSF shall be capable of performing the following management functions: [

4. enable/disable [assignment: all radios on TSF]
5. enable/disable [assignment: all audio or visual collection devices on TSF]
14. remove imported X.S09v3 certificates and [assignment: all other X.509v3 certificates] in the Trust Anchor Database.
20. enable/disable [assignment: all protocols where the device acts as a server].

34. enable/disable device messaging capabilities,
36. enable/disable voice command control of device functions,
41. configure the unlock banner.

FPT_BBD_EXT.l .l: Code executing on any baseband processor (BP) shall not be able to access application processor (AP) resources except when mediated by the AP.

FTA_TAB.1.1: Before establishing a user session, the TSF shall display an Administrator-specified advisory notice and consent warning message regarding use of the TOE.